

THE BRAID GROUP OF \mathbb{Z}^n

DAAN KRAMMER

ABSTRACT. We define pseudo-Garside groups and prove a theorem about them parallel to Garside's result on the word problem for the usual braid groups. The main novelty is that the set of *simple* elements can be infinite. We introduce a group $B = B(\mathbb{Z}^n)$ which we call the braid group of \mathbb{Z}^n , and which bears some vague resemblance to mapping class groups. It is to $\mathrm{GL}(n, \mathbb{Z})$ what the braid group is to the symmetric group S_n . We prove that B is a pseudo-Garside group. We give a *small presentation* for $B(\mathbb{Z}^n)$ assuming one for $B(\mathbb{Z}^3)$ is given.

CONTENTS

1. Introduction	1
2. Lattices of total orderings	3
2.1. The set-theoretic version	3
2.2. Group actions on X	4
2.3. Lexicographic orderings	5
2.4. Proof of lemma 12	5
3. The braid group of \mathbb{Z}^n	7
3.1. Notation and basics	7
3.2. Proof of lemma 27	8
4. Pseudo-Garside groups	9
4.1. Summary	9
4.2. Proofs	10
5. A small presentation for B^+	14
References	21

1. INTRODUCTION

Let S be a compact oriented connected real 2-manifold and p a base point on the boundary of S . To keep things simple, let us define the *mapping class group* M of (S, p) as the group of automorphisms of $F := \pi_1(S, p)$ coming from self-homeomorphisms of S which fix p . Then M acts on $F/F' = H_1(S, \mathbb{Z})$. The kernel I of this action is known as the Torelli group. We have an exact sequence

$$1 \longrightarrow I \longrightarrow M \longrightarrow \mathrm{Aut}(F/F').$$

In general, M/I is infinite, and it is the symplectic group over the integers in the typical case where S has just one boundary component.

If S is a disk with n holes then $M = B_n$, the braid group on n strands. In this case, the Torelli group is also known as the pure braid group P_n . The quotient B_n/P_n is finite (the symmetric group). Perhaps surprisingly, the pure

Date: 31 January 2007.

2000 *Mathematics Subject Classification.* Primary 20F60; secondary 06F15, 20F05, 20F36, 20H05.

braid group turns out to play a pivotal role in algebraically flavoured theories about B_n , for example Garside's greedy forms for braids [Gar69] and finite type invariants [MW02].

It would be interesting to generalise such theories to general mapping class groups M , see [Par05]. There are reasons why the role of the pure braid is expected to be taken by the Torelli group, especially Hain's infinitesimal presentation of the Torelli group [Hai97]. It seems hard to generalise Garside's theory to mapping class groups, which is why I propose to start at the other end. Which groups allow Garside type greedy forms and look a bit like mapping class groups?

Here is a geometric approach, which we don't pursue but may be helpful to think of. The braid group B_n is the fundamental group of the space of n -element subsets of \mathbb{C} . Let A be the fundamental group of the space of additive subgroups of \mathbb{C} isomorphic to \mathbb{Z}^n . This group looks like the braid group: there are points moving around in the plane which aren't allowed to collide. We also have a surjection $A \rightarrow \mathrm{GL}(n, \mathbb{Z})$ which is similar to the surjection $M \rightarrow M/I$.

Now A seems less interesting. For one thing, it is huge and certainly not finitely generated. Which leads us to an algebraic approach.

The weak Bruhat ordering $<$ on the symmetric group S_n is defined by $a \leq ab$ if and only if, for all $i, j \in \{1, \dots, n\}$

$$(i < j \text{ and } iab < jab) \Rightarrow ia < ja. \quad (1)$$

The braid group B_n can be presented by generators $\{r(a) \mid a \in S_n\}$ and relations $r(ab) = (ra)(rb)$ whenever $a \leq ab$.

Let $<$ be the standard lexicographic ordering on \mathbb{Z}^n . In analogy to (1), define an ordering-like relation \lesssim on $G := \mathrm{GL}(n, \mathbb{Z})$ by $a \lesssim ab$ if and only if, for all $x, y \in \mathbb{Z}^n$,

$$(x < y \text{ and } xab < yab) \Rightarrow xa < ya.$$

We define the braid group of \mathbb{Z}^n , written $B = B(\mathbb{Z}^n)$, by generators $\{r(a) \mid a \in G\}$ and relations $r(1) = 1$ and $r(ab) = (ra)(rb)$ whenever $a \lesssim ab$. Taken as a monoid presentation it yields the braid monoid B^+ of \mathbb{Z}^n .

The similarity between B and the usual braid group B_n is obvious. We have a surjection $B \rightarrow \mathrm{GL}(n, \mathbb{Z})$ which reminds us of $M \rightarrow M/I$.

Our first main result is parallel to Garside's greedy form for braids and states that B satisfies the conclusion of theorem 45.

The braid group of \mathbb{Z}^n is an example of what one may call *pseudo-Garside group* which is neither weaker nor stronger than what is called *Garside group* in [Deh02]. We define pseudo-Garside groups in definition 31. Our second main result is that, again, Garside's theory can be generalised to pseudo-Garside groups (see theorem 45). Of course, the paper deals with pseudo-Garside groups in general before it does the braid group of \mathbb{Z}^n .

There are two reasons why one needs different techniques for B than for B_n . The first reason is that in fact, \lesssim is not an ordering but what is known as a preordering. It turns out that this doesn't make the theory much different. The second and chief reason is that $G = \mathrm{GL}(n, \mathbb{Z})$ is infinite, and indeed, has infinite chains. This makes it harder or impossible to use an approach based on a small presentation as is used in [Deh02] and other papers. Instead, we use the generators $r(a)$ from the beginning — even in the definition of the braid group of \mathbb{Z}^n as we saw. We need to build a theory of pseudo-Garside groups up from the ground which we do in section 4.

Our third main result theorem 73 gives (in a precise sense) a presentation of $B^+(\mathbb{Z}^n)$ provided one knows one for $B^+(\mathbb{Z}^3)$. This result is similar to a result by Magnus [Mag34] which gives a presentation of $\mathrm{GL}(n, \mathbb{Z})$ provided one knows one for $\mathrm{GL}(3, \mathbb{Z})$. It is also analogous to the usual presentation (found by Artin) for the usual braid group.

It would be interesting to know if the braid group of \mathbb{Z}^n has any use. Can the mapping class group be embedded in it?

In section 4 we study pseudo-Garside groups. In section 2 we prove enough results to conclude that B (which is defined in section 3) is an example of a pseudo-Garside group. In section 5 we obtain the small presentation for B^+ .

2. LATTICES OF TOTAL ORDERINGS

It is known that the weak Bruhat order (1) on the symmetric group S_n is a lattice ordering. In this section, we state and prove some analogous results. The main result of this section, and the only one needed in the sequel, is proposition 13, and states that some ordering on the set of so-called lexicographic orderings on \mathbb{Z}^n makes it into a lattice.

In the first subsection we make a lattice out of the total orderings on a set. In the second subsection we specialise this by introducing a group action. In the third subsection we specialise even further and look at lexicographic orderings on \mathbb{Z}^n .

2.1. The set-theoretic version. Let X be a set. We write the set of total orderings on X as

$$\{\leq_p \mid p \in P\}$$

where P is an index set. We assume there is no repetition: $\leq_p \neq \leq_q$ whenever $p \neq q$. As usual each of these orderings \leq_p comes with three more relations \geq_p , $<_p$ and $>_p$ whose meanings should be clear. We say that $p \in P$ has some property if \leq_p has.

For $p \in P$ write $R_p = \{(x, y) \in X^2 \mid x <_p y\}$ (which equals $<_p$). Define

$$\begin{aligned} L_p: P &\longrightarrow 2^{R_p}, \\ q &\longmapsto \{(x, y) \in R_p \mid x >_q y\} = R_p \setminus R_q. \end{aligned}$$

The image of L_p is written $L_p(P)$. In this subsection we fix $p \in P$ and write $<, R, L$ instead of $<_p, R_p, L_p$.

Definition 2. Call a set $A \subset R$ *closed* if for all $x, y, z \in X$ with $x < y < z$ one has

$$(x, y) \in A \text{ and } (y, z) \in A \implies (x, z) \in A.$$

Call it *co-closed* if $R \setminus A$ is closed.

Lemma 3. *The map $L: P \rightarrow 2^R$ is injective and its image is the set of closed, co-closed subsets of R .*

Proof. Proof of injectivity of L . Let $q, r \in P$ be distinct. Then there are $x, y \in P$ with $x <_q y$ and $x >_r y$. We may assume $x <_p y$ (otherwise interchange (x, q) with (y, r)). Then $(x, y) \notin L(q)$ and $(x, y) \in L(r)$. This proves that L is injective.

It is readily clear that $L(q)$ is closed and co-closed, for any q .

Let $A \subset R$ be closed and co-closed. We prove that $A \in L(P)$. Define a relation $<$ on X by

$$x < y \Leftrightarrow [(x <_p y \text{ and } (x, y) \notin A) \text{ or } (y <_p x \text{ and } (y, x) \in A)].$$

A tedious case by case proof which we leave to the reader shows that $<$ is transitive. It follows readily that $<$ is an (anti-reflexive) total ordering. So $< = <_q$ for some $q \in P$. Then $A = L(q)$ as required. \square

Definition 4. Define an ordering $\leq = \leq^p$ on P by

$$q \leq r \iff (\text{for all } x, y \in X: x <_p y \text{ and } x <_r y \implies x <_q y). \quad (5)$$

For $p \in P$ we define \bar{p} by $\leq_p = \geq_{\bar{p}}$. It is clear that

$$\leq^p = \geq^{\bar{p}}. \quad (6)$$

Lemma 7. *Let $p, q, r \in P$. Then $q \leq^p r$ if and only if $L_p(q) \subset L_p(r)$.*

Proof. Easy and left to the reader. \square

A *lattice* is an ordered set such that any two elements x, y have a least common upper bound or *join* $x \vee y$ and a greatest common lower bound or *meet* $x \wedge y$. A *complete lattice* is an ordered set such that any subset has a join and a meet.

Proposition 8. *Let $p \in P$. The ordered set (P, \leq^p) is a complete lattice. For any subset $Q \subset P$, the set $L(\vee Q)$ is the closed subset of R generated by $\cup_{q \in Q} L(q)$.*

Proof. By lemmas 3 and 7 we have an isomorphism of ordered sets $L: P \rightarrow L(P)$ where $L(P)$ is ordered by inclusion. We shall prove that $L(P)$ is a lattice.

By lemma 3, $L(P)$ is the set of closed and co-closed subsets $A \subset R$. This is how we think of $L(P)$.

Let $M \subset L(P)$ be any subset. Let B be the union of all elements of M and let C be the closure of B . Equivalently, for $(x, y) \in R$ we have $(x, y) \in C$ if and only if there exist $x = t_0 < t_1 < \dots < t_n = y$ such that $(t_i, t_{i+1}) \in B$ for all i .

It remains to prove that C is a join for M , because meets will follow through the symmetry $\leq^p = \geq^{\bar{p}}$ in (6). Even less is enough, namely, to prove that C is co-closed.

Let $x < y < z$ ($x, y, z \in X$) and suppose $(x, z) \in C$. We want to prove $(x, y) \in C$ or $(y, z) \in C$. By construction there are $x = t_0 < \dots < t_n = z$ such that $(t_i, t_{i+1}) \in B$ for all i .

Suppose first $t_i = y$ for some i . Then $(x, y) = (t_0, t_i) \in C$.

Suppose next $t_i < y < t_{i+1}$ for some i . We know that $(t_i, t_{i+1}) \in A$ for some $A \in M$. As A is co-closed, it contains (t_i, y) or (y, t_{i+1}) , say, $(t_i, y) \in A$. Since $(x, t_i) = (t_0, t_i) \in C$ and $(t_i, y) \in A \subset C$ and C is closed we conclude $(x, y) \in C$. The other case is similar and this proves that C is co-closed as required. \square

By taking X to be finite in proposition 8 one recovers that the weak Bruhat order (1) on the symmetric group is a lattice.

2.2. Group actions on X . We retain the notation of the previous subsection, except that we won't assume any $p \in P$ to be fixed.

The following is obvious.

Lemma 9. *Let g be a permutation of X . If $p, q, r \in P$ are g -invariant then so are $q \vee_p r$ and $q \wedge_p r$.* \square

From now on we assume that $X = \mathbb{Z}^n$ where $n \geq 0$. An element $p \in P$ is said to be *translation invariant* if $x + z <_p y + z \Leftrightarrow x <_p y$ for all $x, y, z \in \mathbb{Z}^n$.

Lemma 10. *Let $p \in P$, $Q \subset P$. If p and all elements of Q are translation invariant then so are $\vee_p Q \in P$ and $\wedge_p Q \in P$ (which are defined by proposition 8).*

Proof. Apply lemma 9, letting g range over all translations $\mathbb{Z}^n \rightarrow \mathbb{Z}^n$, $x \mapsto x + y$ where $y \in \mathbb{Z}^n$. \square

2.3. Lexicographic orderings. We write $G = \text{GL}(n, \mathbb{Z})$ which acts on \mathbb{Z}^n on the right.

Definition 11 (Lexicographic). Let e_1, \dots, e_n be the standard basis of \mathbb{Z}^n . We define the *standard lexicographical ordering* \leq_ℓ on \mathbb{Z}^n as follows.

$$y + \sum_{i=1}^n x_i e_i >_\ell y \iff 0 = x_1 = \dots = x_{i-1} < x_i \text{ for some } i.$$

This ordering is total and translation invariant. We call $p \in P$ *lexicographic* if there exists $g \in G$ such that $x <_p y \Leftrightarrow xg <_\ell yg$ for all $x, y \in \mathbb{Z}^n$.

Lemma 12. *Let $p, q, r \in P$. If p, q, r are lexicographic then so are $q \vee_p r$ and $q \wedge_p r$.*

Proof. See subsection 2.4. \square

Lemma 10 says that if $p \in P$ is translation invariant, then the set of translation invariant elements of P is a complete sublattice of $(P, <^p)$. In particular, it is itself a complete lattice. Likewise, lemma 12 implies the following.

Proposition 13. *Let $p \in P$ be lexicographic. Then the set of lexicographic elements of P has a lattice ordering $<^p$.* \square

It is easy to show that the lattice of proposition 13 is not complete in general.

2.4. Proof of lemma 12. In this subsection we sketch a proof of lemma 12. It can be skipped on first reading.

The *standard lexicographic ordering* $<_\ell$ and the *lexicographic orderings* on \mathbb{Q}^n are defined just as for \mathbb{Z}^n in definition 11. Let $H_{\mathbb{Q}} \subset \text{GL}(n, \mathbb{Q})$ denote the group of linear automorphisms of \mathbb{Q}^n preserving $<_\ell$; it is the group of upper triangular matrices in $\text{GL}(n, \mathbb{Q})$ with positive entries on the diagonal.

Lemma 14. (a). *We have $\text{GL}(n, \mathbb{Q}) = \text{GL}(n, \mathbb{Z}) \cdot H_{\mathbb{Q}}$, that is, every element of $\text{GL}(n, \mathbb{Q})$ can be written xy with $x \in \text{GL}(n, \mathbb{Z})$ and $y \in H_{\mathbb{Q}}$.*

(b). *There is a bijection from the set of lexicographic orderings on \mathbb{Q}^n to those on \mathbb{Z}^n , defined by $< \mapsto < \cap (\mathbb{Z}^n \times \mathbb{Z}^n)$.*

Proof. Part (b) is immediate from (a).

Proof of (a). The inclusion \supset is clear. We prove \subset by induction on n . For $n = 0$ there is nothing to prove. Assume it is true for $n - 1$ and let $g \in \text{GL}(n, \mathbb{Q})$. The \mathbb{Z} -module generated by the entries of the first column of g is of the form $a\mathbb{Z}$ ($a \in \mathbb{Q}_{>0}$). We may suppose that the first column of g is zero, except that $g_{11} = a$ (if not, multiply g on the left with a suitable element

of $\text{GL}(n, \mathbb{Z})$). By the induction hypothesis there are x, y such that $g = xy$, and $y \in H_{\mathbb{Q}}$, and $x \in \text{GL}(n, \mathbb{Z})$ preserves e_1 and $\mathbb{Z}e_2 \oplus \cdots \oplus \mathbb{Z}e_n$. This finishes the proof of (a). \square

Let $f: \mathbb{Q}^n \rightarrow \mathbb{Q}$ be \mathbb{Q} -linear and nonzero. Then $\{x \in \mathbb{Q}^n \mid f(x) > 0\}$ and $\{x \in \mathbb{Q}^n \mid f(x) \geq 0\}$ are called (respectively, open and closed) *half-spaces*. A *PL convex* set is an intersection of finitely many half-spaces (open or closed). Here PL stands for piecewise linear which should not be confused with piecewise affine. A subset of \mathbb{Q}^n is said to be PL if it is a finite union of PL convex sets.

The following result is standard although I can't seem to find a reference.

Proposition 15. *Let $A, B \subset \mathbb{Q}^n$. If A, B are PL then so are $\mathbb{Q}^n \setminus A$, $A \cup B$ and $A + B := \{a + b \mid a \in A, b \in B\}$.* \square

A total translation invariant ordering $<$ on a \mathbb{Q} -vector space V is called Archimedean if for all $x, y \in V$, if $x > 0$ then $kx > y$ for some positive integer k . Equivalently, $(V, <)$ is isomorphic to a \mathbb{Q} -subspace of the real numbers with their standard ordering.

Lemma 16. *Let $<$ denote a translation invariant total ordering on \mathbb{Q}^n . Then there exists a direct decomposition $\mathbb{Q}^n = V_1 \oplus \cdots \oplus V_k$ and Archimedean orderings $<_i$ on V_i such that the following holds. For all $v = \sum_{i=1}^k v_i$ ($v_i \in V_i$) one has $v > 0$ if and only if there exists i with*

$$0 = v_1 = \cdots = v_{i-1} <_i v_i. \quad (17)$$

Proof. This is well-known but I can't seem to find a reference. It is also easily proved by the reader. \square

For $p, q \in P$ translation invariant write

$$\begin{aligned} K(p) &:= \{x \in \mathbb{Q}^n \mid x >_p 0\}, \\ U_p(q) &:= \{x \in \mathbb{Q}^n \mid x >_p 0, x <_q 0\} = K(p) \setminus K(q), \\ U_p^0(q) &:= U_p(q) \cup \{0\}. \end{aligned}$$

From proposition 8 it follows that

$$U_p^0(q \vee_p r) = U_p^0(q) + U_p^0(r). \quad (18)$$

Lemma 19. *Let $p \in P$ be translation invariant, and suppose that $K(p)$ is PL. Then p is lexicographic.*

Proof. Let $<_0$ be the ordering on \mathbb{Q}^n defined by $x <_0 y$ if and only if $nx <_p ny$ for some integer $n > 0$.

By the classification of translation invariant total orderings on \mathbb{Q}^n , lemma 16, there is a direct decomposition $\mathbb{Q}^n = V_1 \oplus \cdots \oplus V_k$ with $V_i \neq 0$ and Archimedean orderings $<_i$ on V_i such that the following holds. For all $v = \sum_{i=1}^k v_i$ ($v_i \in V_i$) one has $v > 0$ if and only if there exists i with (17).

In order to prove the lemma suppose that, to the contrary, the ordering $<_p$ on \mathbb{Z}^n is not lexicographic. By lemma 14(b), $<_0$ isn't lexicographic either. Therefore, there exists j such that $\dim V_j > 1$. Choose a 2-dimensional subspace $W \subset V_j$. Then $K_0(p) := K(p) \cap W$ is PL because $K(p)$ is.

There exists a basis (w_1, w_2) for W and an irrational real number $\alpha \in \mathbb{R}$ such that

$$K_0(p) = \{xw_1 + yw_2 \mid x, y \in \mathbb{Q}, x + \alpha y > 0\}.$$

On writing ∂ for the topological boundary for subsets of $W \otimes_{\mathbb{Q}} \mathbb{R}$ and a bar for closures, it follows that

$$\left(\partial \overline{K_0(p)}\right) \cap W = \{xw_1 + yw_2 \mid x, y \in \mathbb{Q}, x + \alpha y = 0\} = \{0\}.$$

Since $K_0(p)$ is PL this implies $K_0(p) = \{0\}$ which is absurd. \square

Proof of lemma 12. Let $p, q, r \in P$ be lexicographic and write $s = q \vee_p r$. By lemma 10, s is translation invariant.

Now $K(p)$ is easily seen to be PL (because p is lexicographic). Similarly for $K(q)$ and $K(r)$. Moreover $U_p^0(q) = \{0\} \cup K(p) \setminus K(q)$ is also PL, by proposition 15. But

$$U_p^0(s) = U_p^0(q) + U_p^0(r)$$

by (18) which is again PL by proposition 15. Now

$$\begin{aligned} K(s) &= \{x \in \mathbb{Q}^n \mid x >_s 0\} \\ &= \{x \in \mathbb{Q}^n \mid x >_s 0, x >_p 0\} \cup \{x \in \mathbb{Q}^n \mid x >_s 0, x <_p 0\} \\ &= [K(p) \setminus U(s)] \cup -U(s) \end{aligned}$$

is PL. By lemma 19, s is lexicographic as required. Use the symmetry (6) to deal with $q \wedge_p r$. \square

3. THE BRAID GROUP OF \mathbb{Z}^n

In this section we introduce the braid group of \mathbb{Z}^n and prove that it is, in the language of definition 31 below, a pseudo-Garside group.

3.1. Notation and basics.

Definition 20 (Preorderings). A *preordering* on a set X is a relation \lesssim satisfying transitivity ($x \lesssim y$ and $y \lesssim z$ imply $x \lesssim z$) and reflexivity ($x \lesssim x$ for all x). It follows that the relation \sim defined by $x \sim y \Leftrightarrow (x \lesssim y \text{ and } x \gtrsim y)$ is an equivalence relation, and the preordering induces an ordering \leq on X/\sim by $[x] \leq [y] \Leftrightarrow x \lesssim y$ where $[x]$ is the \sim -class of x .

Two totally ordered sets of the same cardinality are not necessarily isomorphic. However, $G = \text{GL}(n, \mathbb{Z})$ acts transitively on the set of *lexicographic* orderings on \mathbb{Z}^n . We'll gratefully make use of this fact which enables us to work with groups rather than groupoids. Groupoids are less convenient in notation though not by concept, and we could have dealt with groupoids had it been necessary.

We give \mathbb{Z}^n the standard lexicographic ordering $<_\ell = <$ (see definition 11). Let H denote the subgroup of G of those elements preserving the ordering on \mathbb{Z}^n .

Recall that the set of total orderings on \mathbb{Z}^n is $\{\leq_p \mid p \in P\}$. We define a map $u: G \rightarrow P$ by

$$0 <_{u(a)} x \iff 0 < xa \quad \text{for all } x \in \mathbb{Z}^n. \quad (21)$$

We define a relation \lesssim on G by

$$a \lesssim ab \iff u(a) \leq u(ab) \quad (22)$$

where \leq denotes \leq^ℓ . So by (5), the definition of \leq^ℓ ,

$$a \lesssim ab \iff (0 < x \text{ and } 0 < xab \Rightarrow 0 < xa \text{ for all } x \in \mathbb{Z}^n). \quad (23)$$

From (22) it is immediate that \lesssim is a preordering on G .

As in definition 20 on preorderings, we define a relation \sim on G by $a \sim ab \iff (a \lesssim ab \text{ and } ab \lesssim a)$. So

$$\begin{aligned} a \sim ab &\iff u(a) \leq u(ab) \leq u(a) \\ &\iff u(a) = u(ab) \iff \angle_{u(a)} = \angle_{u(ab)} \\ &\iff (0 < xa \iff 0 < xab \text{ for all } x \in \mathbb{Z}^n) \\ &\iff b \in H. \end{aligned} \quad (24)$$

So $G/\sim = G/H$. As in definition 20, we have an ordering \leq on $G/\sim = G/H$ given by $aH \leq bH \iff a \lesssim b$.

Lemma 25. *The ordered set $(G/H, \leq)$ is a lattice with least element H and greatest element $w_0 H$ where $w_0 = -1 \in G$. For all $a, b \in G$ one has $a \lesssim b \iff w_0 a w_0^{-1} \lesssim w_0 b w_0^{-1}$.*

Proof. The bit involving w_0 is easy. The rest is just a reformulation of proposition 13. \square

Definition 26. For $a, b \in G$ we write

$$a * b = \begin{cases} ab & \text{if } a \lesssim ab \\ \text{not defined} & \text{otherwise.} \end{cases}$$

Lemma 27. *Let $a, b, c \in G$. Then $(a * b) * c$ is defined if and only if $a * (b * c)$ is.*

Proof. See subsection 3.2. \square

In the language of definition 30 below, we have proved that (G, H, \leq, w_0) is a pseudo-Garside germ.

The definition of the *braid monoid* B^+ of \mathbb{Z}^n and the *braid group* B of \mathbb{Z}^n is given in definition 31 below (it is put there because it can have a wider setting).

3.2. Proof of lemma 27. This subsection is devoted to a proof of lemma 27 and can be skipped in a first reading.

For $a \in G$ we write

$$N(a) = \{x \in \mathbb{Z}^n \setminus \{0\} \mid 0 < x \iff 0 > xa\}.$$

For any two sets A, B we write $A \oplus B$ for the set of elements in A or B but not both.

Lemma 28. *For $a, b \in G$ we have $N(ab) = N(a) \oplus N(b) a^{-1}$.*

Proof. Let $x \in \mathbb{Z}^n$, $x > 0$. Then

$$\begin{aligned} x &\in N(a) \oplus N(b) a^{-1} \\ &\iff [(0 < x \iff 0 > xa) \text{ or } (0 < xa \iff 0 > xab) \text{ but not both}] \\ &\iff [(0 > xa) \text{ or } (0 < xa \iff 0 > xab) \text{ but not both}] \\ &\iff 0 > xab \iff x \in N(ab). \end{aligned}$$

As $N(a) = -N(a)$ a similar result holds for negative x and the proof is finished. \square

Lemma 29. *Let $a, b \in G$. Then the following are equivalent.*

- (1) $a \lesssim b$.
- (2) $N(ab) = N(a) \sqcup N(b) a^{-1}$.
- (3) $N(ab) = N(a) \sqcup N(b) a^{-1}$ (disjoint union).
- (4) $N(a) \cap N(b) a^{-1} = \emptyset$.

Proof. By lemma 28, (2), (3) and (4) are equivalent. The equivalence of (4) and (1) follows from

$$\begin{aligned}
 & N(a) \cap N(b) a^{-1} = \emptyset \\
 \iff & \nexists x \in \mathbb{Z}^n: (0 < x \Leftrightarrow 0 > xa) \text{ and } (0 < xa \Leftrightarrow 0 > xab) \\
 \iff & \nexists x \in \mathbb{Z}^n: 0 < x \Leftrightarrow 0 > xa \Leftrightarrow 0 < xab \\
 \iff & \text{for all } x \in \mathbb{Z}^n: (0 < x \text{ and } 0 < xab) \Rightarrow 0 < xa \\
 \iff & a \lesssim ab,
 \end{aligned}$$

the last equivalence using (23). \square

Proof of lemma 27. We have

$$\begin{aligned}
 & (a * b) * c \text{ is defined} \iff a \lesssim ab \text{ and } ab \lesssim abc \\
 \stackrel{A}{\iff} & N(ab) = N(a) \sqcup N(b) a^{-1} \text{ and } N(abc) = N(ab) \sqcup N(c) (ab)^{-1} \\
 \stackrel{B}{\iff} & N(abc) = N(a) \sqcup N(b) a^{-1} \sqcup N(c) (ab)^{-1} \\
 \stackrel{B}{\iff} & N(bc) = N(b) \sqcup N(c) b^{-1} \text{ and } N(abc) = N(a) \sqcup N(bc) a^{-1} \\
 \stackrel{A}{\iff} & b \lesssim bc \text{ and } a \lesssim abc \iff a * (b * c) \text{ is defined}
 \end{aligned}$$

where A indicates that we use (1) \Leftrightarrow (3) in lemma 29 and B that we use (4) \Rightarrow (3). \square

4. PSEUDO-GARSIDE GROUPS

4.1. Summary.

Definition 30. A *pseudo-Garside germ* is a tuple (G, H, \leq, w_0) with the following properties.

- (PG1) Firstly, $H \subset G$ are groups, and \leq is an ordering on G/H . We write $a \lesssim b \Leftrightarrow aH \leq bH$ ($a, b \in G$) and $a \sim b \Leftrightarrow aH = bH$. We require that \leq is a lattice-ordering on G/H with least element H and greatest element w_0H . For $a, b \in G$ we write

$$a * b = \begin{cases} ab & \text{if } a \lesssim ab \\ \text{not defined} & \text{otherwise.} \end{cases}$$

We call $(x_1, \dots, x_k) \in G^k$ *minimal* if $x_1 * \dots * x_k$ exists.¹

- (PG2) Let $a, b, c \in G$. Then $(a * b) * c$ is defined if and only if $a * (b * c)$ is.

- (PG3) For all $a, b \in G$ one has $a \lesssim b \Leftrightarrow w_0 a w_0^{-1} \lesssim w_0 b w_0^{-1}$.

¹This is rather analogous to what [Bou68] calls *reduced decompositions* of elements of a Coxeter group.

Definition 31. With a pseudo-Garside germ (G, H, \leq, w_0) we associate a monoid B^+ presented as follows.

Generators: $\Omega = \{r(a) \mid a \in G\}$ (a copy of G).

Relations: $r(ab) = (ra)(rb)$ whenever $a, b \in G$ and $a * b$ is defined, that is, $a \lesssim ab$. Also, $r(1) = 1$.

By B we denote the group with the same presentation, taken as group presentation. We put $\Delta = rw_0$. We call B^+ a *pseudo-Garside monoid* and B a *pseudo-Garside group*. Note that Garside groups in the sense of [Deh02] are not necessarily pseudo-Garside groups.

One of the main results of this section is theorem 45 which says the following. In the above notation, every element of B can be written $\Delta^k x_1 \cdots x_\ell$ with $k \in \mathbb{Z}$, $\ell \geq 0$, $(x_1, \dots, x_\ell) \in \Omega^\ell$ *strongly greedy* (see definition 43) and $x_1 \not\sim \Delta$ if $\ell > 0$. Moreover, k is unique and (x_1, \dots, x_ℓ) is unique up to *strong equivalence* (see the beginning of subsection 4.2 for the missing definitions). This is very similar to one of Garside's results on the braid group [Gar69].

In section 3 we proved that the braid group of \mathbb{Z}^n is pseudo-Garside, so that it satisfies, for example, the conclusion of theorem 45.

Of course, every group G is pseudo-Garside: put $H = G$ so that also $B = G$. The challenge is to get H small. In the case of the braid group of \mathbb{Z}^n , the group H is nilpotent and therefore small for many purposes.

The remainder of this section is devoted to the proofs.

4.2. Proofs. In this section we fix a pseudo-Garside germ (G, H, \leq, w_0) and we retain the notation of definitions 30 and 31.

Definition 32. Let G^* be the free monoid on the set G . In order to keep the notation unambiguous, we identify G^* with the disjoint union of Cartesian powers $\cup_{n \geq 0} G^n$. The unique element of G^0 is written \emptyset or $()$. Elements of G^1 are often written (a) rather than a if $a \in G$.

On G^* we define a relation \rightarrow by

$$\rightarrow := \left\{ (u(a)(b * c)v, u(a * b)(c)v) \mid \begin{array}{l} u, v \in G^*, a, b, c \in G, \\ a * b, b * c \text{ defined} \end{array} \right\}.$$

Let \lesssim denote the reflexive-transitive closure of \rightarrow . Clearly, \lesssim is a preordering on G^* . Let \sim denote the associated equivalence relation: $x \sim y \Leftrightarrow x \lesssim y \lesssim x$. Let \approx denote the equivalence relation generated by \rightarrow . In order to distinguish \sim from \approx , we call \approx the *equivalence* and \sim the *strong equivalence*.

It is clear that $x \sim y \Rightarrow x \approx y$ ($x, y \in G^n$). One shouldn't confuse the preordering \lesssim on G^1 (special case of G^n) with the preordering \lesssim on G as in (PG1).

Note that an element of G^n is strongly equivalent to (x_1, \dots, x_n) if and only if it is of the form

$$(x_1 h_1^{-1}, h_1 x_2 h_2^{-1}, h_2 x_3 h_3^{-1}, \dots, h_{n-2} x_{n-1} h_{n-1}^{-1}, h_{n-1} x_n)$$

for some $h_i \in H$.

Warning: If $x \rightarrow y$ with $x \in G^m$ and $y \in G^n$ then $m = n$. The empty word $\emptyset \in G^0$ is *not* equivalent to $(1) \in G^1$. Only later will we identify the two.

Lemma 33. Let $a, b \in G$. Then $a \lesssim ab \Leftrightarrow b \lesssim a^{-1}w_0$. □

Proof. For all $x \in G$, the expression $x * (x^{-1}w_0)$ is defined (and equals w_0) because w_0 is a greatest element. Therefore

$$\begin{aligned} a \lesssim ab &\iff a * b \text{ is defined} \iff (a * b) * (b^{-1}a^{-1}w_0) \text{ is defined} \\ &\iff a * (b * (b^{-1}a^{-1}w_0)) \text{ is defined} \\ &\iff b * (b^{-1}a^{-1}w_0) \text{ is defined} \iff b \lesssim a^{-1}w_0. \end{aligned} \quad \square$$

Lemma 34. *Let $a, b, c, d \in G$ be such that $bH \vee cH = dH$. If $a * b$ and $a * c$ are defined then so is $a * d$.*

Proof. We have $a \lesssim ab$ so, by lemma 33, $b \lesssim a^{-1}w_0$. Similarly, $c \lesssim a^{-1}w_0$. Therefore $d \lesssim a^{-1}w_0$. Using lemma 33 backwards yields $a \lesssim ad$ and therefore $a * d$ is defined. \square

Lemma 35. *Let $u, v, w \in G^*$, $u \rightarrow v$, $u \rightarrow w$. Then there exists $x \in G^*$ such that $v \rightarrow x$, $w \rightarrow x$.*

$$\begin{array}{ccc} u & \longrightarrow & v \\ \downarrow & & \downarrow \\ w & \longrightarrow & x \end{array}$$

Proof. First, consider the case $u = pu_0q$, $v = pv_0q$, $w = pw_0q$ where $u_0, v_0, w_0 \in G^2$, $p, q \in G^*$. We may suppose $p = q = \emptyset$. Write $u = (a, b)$.

As $u \rightarrow v$ we have

$$u = (a, c * d) \rightarrow (a * c, d) = v$$

for some $c, d \in G$. Likewise we can write

$$u = (a, e * f) \rightarrow (a * e, f) = w.$$

Write $r = c \vee e$, $r = c * p = e * q$, $b = r * s$. Since $r * s = (c * p) * s$ is defined, so is $p * s$. In fact, $cd = b = rs = cps$ so $d = p * s$. By lemma 34, $a * r$ is defined, so $a * (c * p)$ is defined. We find

$$v = (a * c, p * s) \rightarrow (a * c * p, s) = (ar, s)$$

and likewise $w \rightarrow (ar, s)$.

Next, consider the “commutative” case

$$u = u_1 u_2 u_3 u_4 u_5, \quad v = u_1 v_0 u_3 u_4 u_5, \quad w = u_1 u_2 u_3 w_0 u_5$$

where $u_2, u_4, v_0, w_0 \in G^2$, $u_1, u_3, u_5 \in G^*$. Then $x := u_1 v_0 u_3 w_0 u_5$ does it.

It remains to consider the case

$$\begin{aligned} u &= p(a, u_2, u_3)q & (a, u_2, u_3) &\in G^3, \\ v &= p(v_1, c, u_3)q & (v_1, c, u_3) &\in G^3, \\ w &= p(a, w_2, e)q & (a, w_2, e) &\in G^3 \end{aligned}$$

with $p, q \in G^*$. We may assume $p = q = \emptyset$. Since $u \rightarrow v$ we have $u_2 = b * c$, $v_1 = a * b$ for some $b \in G$. As $u \rightarrow w$ we have $u_3 = d * e$, $w_2 = u_2 * d = (b * c) * d$ for some $d \in G$. In particular, $(b * c) * d$ is defined. By (PG2), $b * (c * d)$ is also defined. So we have the diagram

$$\begin{array}{ccc} u = (a, b * c, d * e) & \longrightarrow & (a * b, c, d * e) = v \\ \downarrow & & \downarrow \\ w = (a, (b * c) * d, e) & & \\ \parallel & & \\ (a, b * (c * d), e) & \longrightarrow & (a * b, c * d, e) \end{array}$$

which finishes the proof. \square

Definition 36. An element $x \in G^n$ is called *greedy* if its strong equivalence class is maximal, that is, $x \rightarrow y$ implies $x \sim y$. We also say that x is a *greedy form* of every element equivalent to it.

Greedy elements (in an equivalence class) are not unique because all elements strongly equivalent to it are also greedy. But this is the only exception to uniqueness as we show now.

Lemma 37. (a). Every equivalence class $C \subset G^n$ has finite upper bounds, that is, for all $u, v \in C$ there exists $w \in C$ with $u \lesssim w$ and $v \lesssim w$.

(b). Every greedy element of G^n is an upper bound (with respect to \lesssim) of all equivalent elements.

Proof. (a). Let $u, v \in G^*$ be equivalent, that is, there exist

$$u = u_0, u_1, \dots, u_n = v, \quad u_i \in G^*$$

such that for all i one has $u_i \rightarrow u_{i+1}$ or $u_{i+1} \rightarrow u_i$. By induction on n , we prove that $\{u, v\}$ has an upper bound.

For $n = 0$ there is nothing to prove. Assume it is true for $n - 1$. Then $\{u_0, u_{n-1}\}$ has an upper bound w . If $u_n \rightarrow u_{n-1}$ then w is an upper bound of u and v , so suppose $u_{n-1} \rightarrow u_n$.

Since $u_{n-1} \lesssim w$ there exists a diagram as follows.

$$\begin{array}{c} u_{n-1} =: x_0 \longrightarrow x_1 \longrightarrow \dots \longrightarrow x_k := w \\ \downarrow \\ v = u_n =: y_0 \end{array} \quad (38)$$

Using lemma 35 recursively, we can extend (38) to a diagram as follows.

$$\begin{array}{ccccccc} u_{n-1} =: x_0 & \longrightarrow & x_1 & \longrightarrow & \dots & \longrightarrow & x_k := w \\ \downarrow & & \downarrow & & & & \downarrow \\ v = u_n =: y_0 & \longrightarrow & y_1 & \longrightarrow & \dots & \longrightarrow & y_k =: z \end{array}$$

So $v \lesssim z$ and also $u = u_0 \lesssim w \lesssim z$.

(b). Immediate from (a). \square

Lemma 39. Let $(1, x_1, \dots, x_n) \leq (y_0, \dots, y_n)$ (both in G^{n+1}) and suppose that (x_1, \dots, x_n) is greedy. Then $y_0 \lesssim x_1$.

Proof. The equivalence class C of $(1, x_1, \dots, x_n)$ contains $x := (x_1, \dots, x_n, 1)$, which is greedy. By lemma 37(b), x is a greatest element in C . But $y := (y_0, \dots, y_n)$ is in C too, so $y \lesssim x$. Therefore $y_0 \lesssim x_1$. \square

Proposition 40. Every equivalence class in G^* has a greedy element.

Proof. Let $A(n)$ denote the statement that every equivalence class in G^n has a greedy element. We begin by proving $A(2)$. We tacitly use (PG2).

Let $(a, b) \in G^2$. Let $x \in G$ be such that $xH = a^{-1}w_0H \wedge bH$. There exists $y \in G$ with $b = x * y$. Now $x \lesssim a^{-1}w_0$ so by lemma 33, $a * x$ is defined. So

$$(a, b) = (a, x * y) \longrightarrow (a * x, y) =: t.$$

In order to prove that t is greedy, suppose $t \rightarrow t'$, say,

$$t = (a * x, y) = (a * x, u * v) \longrightarrow ((a * x) * u, v) = t'.$$

We have $b = x * y = x * (u * v) = (x * u) * v$ whence

$$x * u \lesssim b. \quad (41)$$

As $a * (x * u)$ is defined we have $x * u \lesssim a^{-1}w_0$ by lemma 33 which we combine with (41) to give

$$a^{-1}w_0H \wedge bH = xH \leq (x * u)H \leq a^{-1}w_0H \wedge bH.$$

Therefore $u \sim 1$. This proves that t is greedy and $A(2)$ is proved.

The proof of $A(n)$ is finished by induction on n . For $n \leq 1$ there is nothing to prove, and $A(2)$ has been proved above. We suppose $A(n-1)$ ($n \geq 3$) and aim to prove $A(n)$.

Let $C \subset G^n$ be an equivalence class. By $A(n-1)$, C contains an element $x = (x_1, \dots, x_n)$ such that (x_2, \dots, x_n) is greedy. By $A(2)$ there exists a greedy element $(y_1, y_2) \approx (x_1, x_2)$. By lemma 39 we have

$$[x \rightarrow (z_1, \dots, z_n)] \Rightarrow z_1 \lesssim y_1. \quad (42)$$

Define $w_1 := y_1$ and let $(w_2, \dots, w_n) \approx (y_2, x_3, \dots, x_n)$ be greedy. Note

$$x \rightarrow (y_1, y_2, x_3, \dots, x_n) \rightarrow w := (w_1, \dots, w_n).$$

In order to prove w to be greedy, assume $w \rightarrow z = (z_1, \dots, z_n)$. By (42) we have $z_1 \sim w_1$ (because $y_1 = w_1 \lesssim z_1 \lesssim y_1$). By greediness of (w_2, \dots, w_n) we get $w \sim z$. So w is greedy and the proof is finished. \square

Definition 43. An element $(x_1, \dots, x_n) \in G^n$ is called *strongly greedy* if it is greedy and $(n \geq 2 \Rightarrow x_n \not\sim 1)$ and $(n = 1 \Rightarrow x_1 \neq 1)$.

We say that an element $(rx_1, \dots, rx_k) \in \Omega^k$ (or two such) has some property (greedy, strongly greedy, equivalent, strongly equivalent) if $(x_1, \dots, x_k) \in G^k$ has.

Theorem 44. Every element of B^+ can be written $x_1 \cdots x_n$ with $n \geq 0$, $x_i \in \Omega$ and (x_1, \dots, x_n) strongly greedy. Moreover, (x_1, \dots, x_n) is unique up to strong equivalence.

Proof. Let \equiv denote the smallest equivalence relation on G^* containing \approx and such that $u(1)v \equiv uv$ for all $u, v \in G^*$. Then $B^+ \cong G^*/\equiv$. We have

$$x \sim y \Rightarrow x \approx y \Rightarrow x \equiv y$$

for all $x, y \in G^*$.

We shall define a map S from G^* to the set of strongly greedy elements in G^* . Let $R(x)$ denote any greedy element with $R(x) \approx x$ (it is not unique but we just choose one). Write $R(x) = (a_1, \dots, a_n)$. If $n \leq 1$ we put $S(x) := R(x)$. If $n \geq 2$, let k be maximal such that $a_k \notin H$ and write $b = a_k \cdots a_n$. We put $S(x) = (a_1, \dots, a_{k-1}, b)$. Then $S(x)$ is strongly greedy and $S(x) \equiv x$. Also, if x is strongly greedy then $x \sim R(x) = S(x)$.

We claim that for all $x, y \in G^*$, if $x \equiv y$ then $S(x) \sim S(y)$. By the definition of \equiv , we need to prove this only if $x = u(1)v$, $y = uv$ (with $u, v \in G^*$) or if $x \approx y$. The case of $x \approx y$ is trivial. Now suppose $x = u(1)v$ and $y = uv$. Then $x \lesssim uv(1) = y(1)$ so $x \approx y(1)$ so $R(x) \sim R(y)(1)$ and $S(x) \sim S(y)$.

Now we can prove the lemma. Existence. Let $x \in G^*$. Then $S(x)$ is strongly greedy and $x \equiv S(x)$ as required.

Uniqueness. Let $x, y \in G^*$ be strongly greedy and $x \equiv y$. Because of $x \equiv y$ we get $S(x) \sim S(y)$. So $x \sim S(x) \sim S(y) \sim y$ as required. \square

Note that we haven't used (PG3) so far. It is used in the proof of the following result.

Theorem 45. *Every element of B can be written $\Delta^k x_1 \cdots x_\ell$ with $k \in \mathbb{Z}$, $\ell \geq 0$, $(x_1, \dots, x_\ell) \in \Omega^n$ strongly greedy and $x_1 \not\sim \Delta$ if x_1 is defined. Moreover, k is unique and (x_1, \dots, x_ℓ) is unique up to strong equivalence.*

Proof. Easy using (PG3) and theorem 44 and left to the reader. \square

5. A SMALL PRESENTATION FOR B^+

The main result in this section is theorem 73 which gives a presentation of B^+ , the braid monoid of \mathbb{Z}^n , in terms of generators and relations. Our approach is quite similar to Magnus' way [Mag34] to present $\text{GL}(n, \mathbb{Z})$ assuming that one has a presentation of $\text{GL}(3, \mathbb{Z})$.

Definition 46. We define G_i ($1 \leq i < n$) to be the group of those $g \in G$ which preserve each e_j ($j \notin \{i, i+1\}$) as well as $\mathbb{Z}e_i \oplus \mathbb{Z}e_{i+1}$. Define $s_i \in G$ ($1 \leq i \leq n$) by $e_i s_i = -e_i$ and $e_j s_i = e_j$ for all $j \neq i$. Note that $G_{i-1} \cap G_i = \langle s_i \rangle$.

Lemma 47. (a). *Let $a \in G$, $b \in H$. Then $a * b$ and $b * a$ are defined.*
 (b). *For all $a \in G_i$ and $x \in H$ there are $b \in G_i$, $y \in H$ such that*

$$ax = yb. \quad (48)$$

(c). *Same as (b) with $xa = by$ instead of (48).*

Proof. (a). Clearly, $a * (b * b^{-1})$ and $(b^{-1} * b) * a$ are defined. By lemma 27, $a * b$ and $b * a$ are defined.

Parts (b) and (c) are easy and left to the reader. \square

Definition 49 (shapes). See figure 1. A *shape* is a set $A \subset \{1, \dots, n\}^2$ such that $(i, i) \in A$ for all i , and for all $(i, j) \in \{1, \dots, n\}^2$

$$(i, j) \notin A \implies (i+1, j) \notin A \text{ and } (i, j-1) \notin A.$$

Let $g \in G$. As usual, g is a matrix $(g_{ij})_{ij}$ where i, j range over $\{1, \dots, n\}$; by definition (since G acts on the right)

$$e_i g = \sum_j g_{ij} e_j.$$

We define $\text{shape}(g)$ (the shape of g) to be the smallest shape A containing $\{(i, j) \mid g_{ij} \neq 0\}$.

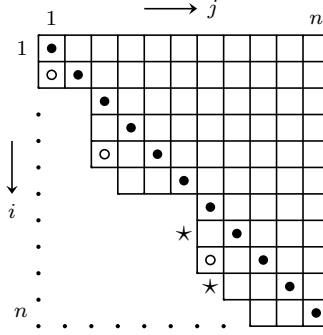
For a shape A , we define $G(A)$ to be the set of those elements of G whose shape is contained in A . Note $H G(A) H = G(A)$. Note also $H \subset G(A_0)$ where A_0 is the smallest shape: $A_0 = \{(i, j) \in \{1, \dots, n\}^2 \mid i \leq j\}$.

Definition 50. Recall $u: G \rightarrow P$ from (21). For $g \in G$ we define $M(g)$ by

$$\begin{aligned} M(g) &= \{x \in \mathbb{Z}^n \mid (0, x) \in L_\ell(u(g))\} = \{x \in \mathbb{Z}^n \mid x > 0, x <_{ug} 0\} \\ &= \{x \in \mathbb{Z}^n \mid x > 0 > xg\} \end{aligned}$$

Lemma 51. *Let $a, b \in G$. Then $a \lesssim ab \Leftrightarrow M(a) \subset M(ab)$.*

FIGURE 1. A shape C . The black dots form the main diagonal. The white dots are the possible positions of $(i+1, j) \in C \setminus A$ in proposition 52. In case $(i+1, j)$ is the lower white dot, the stars are the positions $(i, j-1)$, $(i+2, j)$ which proposition 52 assumes not to be in A .



Proof. We have

$$\begin{aligned}
 a &\lesssim ab \stackrel{(23)}{\iff} (\text{for all } x \in \mathbb{Z}^n: 0 < x \text{ and } 0 < xab \Rightarrow 0 < xa) \\
 &\iff \{x \in \mathbb{Z}^n \mid x > 0 > xa\} \subset \{x \in \mathbb{Z}^n \mid x > 0 > xab\} \\
 &\iff M(a) \subset M(ab). \quad \square
 \end{aligned}$$

Proposition 52. See figure 1. Let $A \subset C$ be shapes with $\#C = \#A + 1$. Suppose $(i+1, j) \in C \setminus A$, $(i, j-1) \notin A$, $(i+2, j) \notin A$. Let $x \in G(C)$.

- (a). There are $y \in G_i$ and $z \in G(A)$ such that $x = y * z$.
- (b). Any other pair (y, z) with the same properties is of the form $(y, z) = (yt, t^{-1}z)$ with $t \in \langle s_{i+1}, H \cap G_i \rangle$.

Proof. (a). If $\text{shape}(x) \subset A$ there is nothing to do (choose $y = 1$, $z = x$), so suppose otherwise, that is, $x_{i+1,j} \neq 0$. Write

$$\begin{pmatrix} x_{ij} \\ x_{i+1,j} \end{pmatrix} = \begin{pmatrix} au \\ bu \end{pmatrix} \tag{53}$$

where $a, b, u \in \mathbb{Z}$ with a, b coprime and $u > 0$. Choose $c, d \in \mathbb{Z}$ such that

$$ad - bc = 1. \tag{54}$$

Define

$$y_0 = \begin{pmatrix} av & cw \\ bv & dw \end{pmatrix} \tag{55}$$

where $v, w \in \{-1, 1\}$ are to be determined later. Note that they are allowed to depend on x . Let $y \in G_i$ be the (unique) element of G_i with y_0 in rows and columns of indices $i, i+1$. Put $z = y^{-1}x$. We need to show $x = y * z$ and $z \in G(A)$.

We shall prove $z \in G(A)$. It is clear that $z = y^{-1}x \in G(C)$; we need to prove $z_{i+1,j} = 0$. Consider the entries (53) in x . The corresponding entries in

z are

$$\begin{aligned} y_0^{-1} \begin{pmatrix} x_{ij} \\ x_{i+1,j} \end{pmatrix} &= y_0^{-1} \begin{pmatrix} au \\ bu \end{pmatrix} = u v w \begin{pmatrix} dw & -cw \\ -bv & av \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \\ &= u v w \begin{pmatrix} w(ad - bc) \\ 0 \end{pmatrix} = \begin{pmatrix} uv \\ 0 \end{pmatrix} \end{aligned}$$

which shows that $z \in G(A)$.

It remains to show $x = y * z$, that is, $y \lesssim x$, or equivalently (by lemma 51) $M(y) \subset M(x)$. Let $t \in M(y)$, that is (by definition 50), $ty < 0 < t$. Write $t = \sum_k t_k e_k$. Note that $t_k = 0$ for $k < i$ because otherwise, t and ty have the same sign, contradicting $ty < 0 < t$. For a similar reason

$$(t_i, t_{i+1}) \neq 0. \quad (56)$$

The i -th and $(i+1)$ -th coefficients of ty are

$$\begin{aligned} ((ty)_i, (ty)_{i+1}) &= (t_i, t_{i+1}) y_0 = (t_i, t_{i+1}) \begin{pmatrix} av & cw \\ bv & dw \end{pmatrix} \\ &= (v(a t_i + b t_{i+1}), w(c t_i + d t_{i+1})) \end{aligned}$$

which is a nonzero vector by (56).

Recall that we have $t > 0$ whose definition simplifies to

$$t_i > 0 \text{ or } (t_i = 0, t_{i+1} > 0). \quad (57)$$

Similarly we have $ty < 0$ whose definition simplifies to

$$v(a t_i + b t_{i+1}) < 0 \text{ or } (a t_i + b t_{i+1} = 0, w(c t_i + d t_{i+1}) < 0). \quad (58)$$

We put $v = 1$. Recall that $b \neq 0$; we assume $w \in \{-1, 1\}$ has the sign of $-b$.

We shall prove

$$a t_i + b t_{i+1} \neq 0. \quad (59)$$

Suppose (59) is false. By (58) we find

$$\begin{aligned} 0 &> b^2 w(c t_i + d t_{i+1}) \\ &= b w(b c t_i + d(b t_{i+1})) \\ &= b w(b c t_i - a d t_i) \quad \text{since not (59)} \\ &= -b w(a d - b c) t_i. \end{aligned}$$

But $-bw > 0$ and $ad - bc = 1$ so $t_i < 0$, contradicting (57). This proves (59). By (58) and (59) we find

$$a t_i + b t_{i+1} < 0. \quad (60)$$

The i -th coefficient of tx is $at_i + bt_{i+1} < 0$ by (60) and all preceding coefficients are zero, so $tx < 0$. Also $t > 0$ so $t \in M(x)$ by definition 50. This proves $M(y) \subset M(x)$ thus proving (a).

(b). We prefer to work with y but not z ; the conditions for y to be satisfied are

$$y \lesssim x \quad (61)$$

and

$$y^{-1}x \in G(A). \quad (62)$$

An easy computation which we leave to the reader shows that y satisfies (62) if and only if there exists $p \in H \cap G_i$ such that yp is of the form (55) for some $v, w \in \{-1, 1\}$ (or rather, its submatrix in rows and columns $i, i+1$). By

lemma 47, (61) is also invariant under multiplying y on the right with elements of $H \cap G_i$.

Assume therefore that y is of the form (55) and satisfies (61). The proof will be finished by showing that $v = 1$.

Suppose the contrary, $v = -1$. Choose $t_i, t_{i+1} \in \mathbb{Q}$ such that $t_i > 0$ and $at_i + bt_{i+1} > 0$, and put $t = t_i e_i + t_{i+1} e_{i+1}$. Then by (57) we have $t > 0$ and by (58) we have $ty < 0$. Therefore $t \in M(y)$. But the i -th coefficient of tx is $at_i + bt_{i+1} > 0$ by (60) and all preceding coefficients are zero, so $tx > 0$ and $t \notin M(x)$. Therefore, $M(y) \not\subset M(x)$, that is, (61) is false. This contradiction finishes the proof. \square

Lemma 63. *Let $x, y \in G$ be diagonal matrices (necessarily all diagonal entries being 1 or -1). Suppose that for all i , if $e_i x = -e_i$ then $e_i y = -e_i$. Then $x \lesssim y$.*

Proof. By lemma 51 we need to prove $M(x) \subset M(y)$. Note $0 \notin M(x)$. Let $v = \sum_i v_i e_i \in \mathbb{Z}^n$, $v \neq 0$, say, $0 = v_1 = \dots = v_{k-1} \neq v_k$. Then

$$\begin{aligned} v \in M(x) &\Leftrightarrow (v > 0, vx < 0) \Leftrightarrow (v_k > 0, e_k x = -e_k) \\ &\Rightarrow (v_k > 0, e_k y = -e_k) \Leftrightarrow (v > 0, vy < 0) \Leftrightarrow v \in M(y). \quad \square \end{aligned}$$

Corollary 64. *The monoid B^+ is generated by*

$$\left(\bigcup_{i=1}^{n-1} rG_i \right) \cup rH. \quad (65)$$

Proof. Let $M \subset B^+$ denote the monoid generated by (65). We know that B^+ is generated by $r(G)$ so we will be done if we prove that $r(x) \in M$ for all $x \in G$. We shall do this by induction on $\# \text{shape}(x)$.

First suppose $\text{shape}(x)$ is minimal, that is, x is upper triangular. It is clear that

$$x = t_1 \cdots t_k h$$

for some $k \geq 0$, some distinct $t_1, \dots, t_k \in \{s_1, \dots, s_n\}$ and some $h \in H$. By lemma 63 it follows that $x = t_1 * \dots * t_k * h$ or equivalently

$$rx = (rt_1) \cdots (rt_k)(rh).$$

But each rt_i is in some $r(G_j)$, thus proving the statement if $\text{shape}(x)$ is minimal.

Assume $\text{shape}(x) = C \neq A_0$ and assume that the result has been proved for all $z \in G$ with $\# \text{shape}(z) < \#C$. The proof will be finished if we can prove the required result for x .

Note that there exist indices i, j and a shape $A \subset C$ satisfying the assumptions of proposition 52. For example, one can choose j to be minimal such that the j -th column of C differs from the j -th column of A_0 ; subject to this, let i be maximal such that $(i, j) \in C$ and put $A = C \setminus \{(i, j)\}$.

By proposition 52 there exist $y \in G_i$, $z \in G(A)$ such that $x = y * z$. Then $rx = (ry)(rz)$. Now $rz \in M$ by the induction hypothesis while $ry \in r(G_i) \subset M$ so $rx \in M$. The proof is finished. \square

We define H_i to be the group generated by G_i and H . By lemma 47, all its elements can be written $a * x$ and $y * b$ ($a, b \in G_i$, $x, y \in H$). We define S to be the union of all H_i . We write $S^* = \cup_{n \geq 0} S^n$. A multiplication in S^* is defined by concatenation, making it into a free monoid on S^1 .

A *congruence* on a monoid M is an equivalence relation \sim on it such that the quotient set M/\sim has a (necessarily unique) monoid structure such that the natural set map $M \rightarrow M/\sim$ is a homomorphism of monoids.

Let \sim denote the smallest congruence on S^* satisfying the following.

- (S0) We have $S^1 \ni (1) \sim \emptyset \in S^0$.
- (S1) We have $(x, y) \sim (xy)$ for all $x, y \in H_i$ such that $x * y$ is defined.
- (S2) We have $(x, y) \sim (y, x)$ whenever $x \in G_i, y \in G_j$ and $|i - j| > 1$.
- (S3) We have $(x_1, y_1, x_2) \sim (y_2, x_3, y_3)$ whenever the following hold.
 - (a) $x_k \in G_i$ for all k .
 - (b) $y_k \in G_{i+1}$ for all k .
 - (c) $x_1 * y_1 * x_2$ and $y_2 * x_3 * y_3$ are defined and equal.

Lemma 66. *Consider the monoid homomorphism $f: S^* \rightarrow B^+$ defined by $f(x) = r(x)$ for all $x \in S^1 = S$. For all $x, y \in S^*$, if $x \sim y$ then $f(x) = f(y)$.*

Proof. Let $x \in G_i, y \in G_j, |i - j| > 1$. Then $xy = yx$. It is easy and left to the reader to prove that $x * y$ and $y * x$ are defined. So $f(x, y) = (rx)(ry) = r(xy) = r(yx) = (ry)(rx) = f(y, x)$. This proves that the map f respects (S2). The other cases (S0), (S1), (S3) are trivial. \square

Our aim is to prove the converse of lemma 66 ($f(x) = f(y) \Rightarrow x \sim y$) which we do in theorem 73.

We write $T = \{1, 2, \dots, n - 1\}$ and $T^* = \cup_{n \geq 0} T^n$ which, as S^* , is a free monoid on T^1 with concatenation as multiplication.

We say that $(x_1, \dots, x_k) \in S^k$ has *type* $(y_1, \dots, y_k) \in T^k$ if $x_i \in H_{y_i}$ for all i . Every word (= element in S^*) has at least one type, but possibly more.

Let \rightarrow be the smallest relation on T^* with the following properties.

- (T0) We have $T^0 \ni \emptyset \rightarrow (i) \in T^1$ for all i .
- (T1) We have $(i, i) \rightarrow (i)$ for all i .
- (T2) We have $(i, j) \rightarrow (j, i)$ whenever $|i - j| > 1$.
- (T3) We have $(i, j, i) \rightarrow (j, i, j)$ whenever $j = i + 1$.
- (T4) We have $axb \rightarrow ayb$ whenever $x \rightarrow y$ ($a, b, x, y \in T^*$).

Notice the similarity with the congruence \sim on S^* . If $t_1 \rightarrow t_2$ we say that t_1 can be *rewritten to* t_2 .

The following lemma ties up S with T .

Lemma 67. *Let $t_1, t_2 \in T^*$ with $t_1 \rightarrow t_2$. Then for every minimal word $w_1 \in S^*$ of type t_1 there exists a minimal word w_2 of type t_2 such that $w_1 \sim w_2$.*

Proof. It is enough to do this in the following cases.

- (0) $T^0 \ni \emptyset = t_1 \rightarrow t_2 = (i) \in T^1$.
- (1) $t_1 = (i, i) \rightarrow (i) = t_2$.
- (2) $t_1 = (i, j) \rightarrow (j, i) = t_2, |i - j| > 1$.
- (3) $t_1 = (i, j, i) \rightarrow (j, i, j) = t_2, j = i + 1$.

Case (0). We have $w_1 = \emptyset \in S^0$. Choose $w_2 = 1$. We have $w_1 \sim w_2$ by (S0).

Case (1). Let $w_1 \in S^*$ be minimal of type (i, i) . Write $w_1 = (x, y)$. By minimality of w_1 then, $x * y$ is defined. So a good choice is $w_2 = (xy)$ by (S1).

Case (2). Let w_1 be minimal and of type $(i, j), |i - j| > 1$. By lemma 47 we can write $w_1 = (xa, by)$ where $x, y \in H, a \in G_i, b \in G_j$. Then $w_1 = (xa, by) \sim (x, a, b, y) \sim (x, b, a, y) \sim (xb, ay)$ so $w_2 = (xb, ay)$ is a good choice.

Case (3). Let $w_1 \in S^*$ be minimal of type (i, j, i) with $j = i+1$. By lemma 47 we can write $w_1 = (a_1x_1, a_2x_2, a_3x_3)$. Using lemma 47 we can separate G_k and H , that is, $w_1 \sim w_3$ for some $w_3 = (b_1, b_2, b_3, y)$ with $b_1, b_3 \in G_i$, $b_2 \in G_j$ and $y \in H$. By proposition 52 applied three times with $n = 3$, we can write $b_1b_2b_3 = c_1 * c_2 * c_3$ for some $c_2 \in G_i$, $c_1, c_3 \in G_j$. Then $w_3 \sim w_2 := (c_1, c_2, c_3y)$ which is of type (j, i, j) as required. \square

Remark 68. Note that case (3) in the proof of lemma 67 would fail if we replaced “ $t_1 \rightarrow t_2$ ” by “ $t_2 \rightarrow t_1$ ”, or equivalently, interchanged i and j in the definition (T3) of \rightarrow . Certainly, proposition 52 fails in that situation.

Lemma 69. *We have*

$$(k, \dots, 1)(k, \dots, 1) \longrightarrow (k, \dots, 1)(k, \dots, 2)$$

whenever $0 < k < n$. (Note that, for example, $(i, j)(k, \ell) \in T^4$ is exactly (i, j, k, ℓ) ; we are using brackets here to ease reading).

Proof. Induction on k . If $k = 1$ it reads $(1, 1) \rightarrow (1)$ and follows from (T1). Suppose it is true for $k - 1$.

In the first arrow labelled (T2) in the following, we push the last k to the left as far as possible using only (T2). Similarly, in the last arrow labelled (T2) the last k is pushed back to the right. We write IH for the induction hypothesis.

$$\begin{aligned} & (k, \dots, 1)(k, \dots, 1) \\ & \xrightarrow{(T2)} (k, k-1, k)(k-2, \dots, 1)(k-1, \dots, 1) \\ & \xrightarrow{(T0)} (k, k-1, k)(k-1, \dots, 1)(k-1, \dots, 1) \\ & \xrightarrow{\text{IH}} (k, k-1, k)(k-1, \dots, 1)(k-1, \dots, 2) \\ & = (k)(k-1, k, k-1)(k-2, \dots, 1)(k-1, \dots, 2) \\ & \xrightarrow{(T3)} (k)(k, k-1, k)(k-2, \dots, 1)(k-1, \dots, 2) \\ & \xrightarrow{(T1)} (k, k-1, k)(k-2, \dots, 1)(k-1, \dots, 2) \\ & \xrightarrow{(T2)} (k, \dots, 1)(k, \dots, 2). \end{aligned} \quad \square$$

For fixed n , we write

$$D_i = (n-1, \dots, i)(n-1, \dots, i+1) \cdots (n-1, n-2)(n-1) \in T^*.$$

Proposition 70. *Any element of T^* can be rewritten to*

$$D_1 = (n-1, \dots, 1)(n-1, \dots, 2) \cdots (n-1).$$

Proof. We use a double induction. Call the statement of the lemma $A(n)$. We prove $A(n)$ by induction on n . We clearly have $A(1)$. Assuming $A(n-1)$, we shall prove $A(n)$. Let $x \in T^k$. We prove $x \rightarrow D_1$ by induction on k .

For $k = 0$ this follows from (T0). Assuming it true for $k - 1$ we prove it for k . Since it is true for $k - 1$ we can write $x = D_1(i)$ (product of D_1 and $(i) \in T^1$). If $i \neq 1$ then $A(n-1)$ tells us that $x = (n-1, \dots, 1) D_2(i)$ can be rewritten to $x = (n-1, \dots, 1) D_2 = D_1$ as required. Suppose now $i = 1$. Pushing the last letter $i = 1$ as far as possible to the left using only (T2) we

get

$$[(n-1, \dots, 1)(n-1, \dots, 1)](n-1, \dots, 3)(n-1, \dots, 4) \cdots (n-1).$$

Rewriting the part in square brackets using lemma 69 yields D_1 as required. \square

Corollary 71. *Every element of G is of the form $x_1 \cdots x_k$ where $(x_1, \dots, x_k) \in S^k$ is minimal of type D_1 .*

Proof. Immediate from corollary 64 and lemmas 67 and 70. \square

Lemma 72. *Let $a \in G_i$. Then a and as_{i+1} are comparable, that is, $a \lesssim as_{i+1}$ or $as_{i+1} \lesssim a$.*

Proof. Easy and left to the reader. \square

Theorem 73. (a). *The converse to lemma 66 holds. In other words, the monoid B^+ is presented by generators S and relations (S0)–(S3).*

(b). *The group B is presented by the same generators and relations, taken as a group presentation.*

Proof. Part (b) follows immediately from (a). We prove (a) by a double induction. Let $A(n)$ denote the statement of the theorem. Then clearly $A(2)$. Assuming $A(n-1)$ we prove $A(n)$ ($n > 2$).

By the definition of B^+ , it suffices to show that for *minimal* words $w_1, w_2 \in S^*$, if $f(w_1) = f(w_2)$ then $w_1 \sim w_2$. In order to keep notation simple, we repeatedly replace w_1, w_2 by equivalent minimal words until they are equal or obviously equivalent.

Let $X: S^* \rightarrow G$ be the natural homomorphism: $X(a) = a$ for all $a \in S^1 = S$. Write $x = (x_{ij}) := X(w_1) = X(w_2) \in G$.

Proposition 70 tells us that any type of w_1 can be rewritten to standard type (that is, type D_1). By lemma 67, w_1 is equivalent to a word of standard type. So we may now assume that w_1 is of standard type, say,

$$w_1 = (y_{n-1}, \dots, y_1) u$$

with $y_i \in H_i$ and $u \in S^*$ of type D_2 . By lemma 47 we may even assume $y_i \in G_i$ (we can collect the necessary H factors in the type D_2 factor u).

Here and henceforth we write $J(w)$ for the greatest j such that the $(j, 1)$ -entry in $X(w)$ is nonzero ($w \in S^*$). Put $j = J(w_1)$.

If $n > k \geq j$ then $y_k y_{k-1} \cdots y_1 X(u)$ has the same first column as x . Now $y_{j-1} \cdots y_1 X(u)$ may have a different first column, but it cannot have a nonzero entry in position $(j+1, 1)$, because that couldn't be cleaned up by removing any number of y_i factors on the left. We may now assume $y_j \in \langle s_{j+1}, s_j \rangle$ (otherwise, move some H factor into the type D_2 factor). Write $y_j = s_{j+1}^p s_j^q$ with $p, q \in \{0, 1\}$. We may assume $y_j = s_j^q \in \langle s_j \rangle$ because otherwise we replace $(y_{j+1}, y_j) = (y_{j+1}, s_{j+1}^p s_j^q)$ by $(y_{j+1} s_{j+1}^p, s_j^q)$. Then y_i and y_k commute whenever $i \leq j < k$. We may now assume $y_k = 1$ for all $k > j$ (otherwise push them to the right into the type D_2 factor). Summarising, we now have $y_k = 1$ for $k > j$ and $y_j \in \langle s_j \rangle$.

We continue the proof by induction on j . First consider the case $j = 1$. Then $x_{11} = (-1)^q$ for some $q \in \{0, 1\}$. Moreover, $w_1 = (s_1^q)u$, for some $u \in S^*$ of type D_2 . Likewise, we have $w_2 = (s_1^q)v$ for some $v \in S^*$ of type D_2 . By $A(n-1)$, we have $u \sim v$ and therefore $w_1 \sim w_2$. This establishes the case where $j = 1$.

Supposing now the result for $j - 1$ and smaller, we prove it for j .

Recall that $y_j \in \langle s_j \rangle \subset G_{j-1}$. We may assume that $y_j = 1$ because otherwise we replace (y_j, y_{j-1}) by $(1, y_j y_{j-1})$. Summarising, we have $w_1 = (y_{j-1}, \dots, y_1) u$. Similarly, we can write $w_2 = (z_{j-1}, \dots, z_1) v$.

Let C be the shape of $x = X(w_1) = X(w_2)$ and $A = C \setminus \{(j, i)\}$ where $i = 1$. Then $y = y_{j-1}$ and $y = z_{j-1}$ both satisfy the conditions of proposition 52, that is, (61) and (62). By proposition 52(b) we must have $z_{j-1} = y_{j-1} s_j^t$ for some $t \in \{0, 1\}$ after moving some H factors around.

We will now show that we may in fact suppose $t = 0$. If not, then $z_{j-1} = y_{j-1} s_j$. By lemma 72, z_{j-1} and y_{j-1} are comparable. After interchanging w_1 and w_2 if necessary, we may assume $y_{j-1} \lesssim z_{j-1}$, that is, $z_{j-1} = y_{j-1} * s_j$. In our word w_2 , replace z_{j-1} by (y_{j-1}, s_j) . Now s_j commutes with everything on its right but not in the type D_2 factor. Push s_j into the type D_2 factor using (T2). Now w_2 is of the form as before except that $z_{j-1} = y_{j-1}$, that is, $t = 0$.

So $w_1 = (y_{j-1})v_1$ and $w_2 = (y_{j-1})v_2$ where $J(v_1)$ and $J(v_2)$ are smaller than $j = J(w_1) = J(w_2)$. By the induction hypothesis we have $v_1 \sim v_2$ and therefore $w_1 \sim w_2$. This proves (a). \square

REFERENCES

- [Bou68] Bourbaki, Nicolas. *Lie groups and Lie algebras. Chapters 4–6*. Translated from the 1968 French original. Springer-Verlag, Berlin, 2002.
- [Deh02] Dehornoy, Patrick. Groupes de Garside. Ann. Sci. École Norm. Sup. (4) **35** (2002), no. 2, 267–306.
- [Gar69] Garside, F. A. The braid group and other groups. Quart. J. Math. Oxford Ser. (2) **20** (1969), 235–254.
- [Hai97] Hain, Richard. Infinitesimal presentations of the Torelli groups. J. Amer. Math. Soc. **10** (1997), no. 3, 597–651.
- [Mag34] Magnus, Wilhelm. Über n -dimensionale Gittertransformationen. Acta Math. **64** (1934), 353–367.
- [MW02] Mostovoy, Jacob; Willerton, Simon. Free groups and finite-type invariants of pure braids. Math. Proc. Cambridge Philos. Soc. **132** (2002), no. 1, 117–130.
- [Par05] Paris, Luis. From braid groups to mapping class groups.
<http://arxiv.org/abs/math.GR/0412024>.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WARWICK, COVENTRY CV4 7AL,
UK

E-mail address: D.Krammer@warwick.ac.uk